In the claims:

This listing of claims will replace all prior versions and listings of claims in the Application.

1. (Currently Amended) Method for detecting fraud in non-personal transactions involving shipment of physical merchandise from a merchant to a potential purchaser, comprising the steps of:

collecting purchaser data for the transaction, said purchaser data comprising a billing address and a ship-to address;

storing said purchaser data on a non-transitory computer readable storage medium;

transmitting said ship-to address to a fraud-detection system;

processing said ship-to address with a computer processor to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to address against non-billing address criteria;

returning the relative risks of fraudulent activity associated with the transaction; and whereby the shipment of the merchandise from the merchant to the purchaser is effected if the relative risks of fraudulent activity associated with the transaction is below the merchant's threshold.

2. (Original) The fraud detection method according to claim 1, wherein the processing step comprising parsing out the purchaser's ship-to address.

3. (Previously Presented) The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises a step of checking to determine whether the purchaser's ship-to address exists.

4. (Previously Presented) The fraud detection according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises comparing a zip code of the ship-to address against a post office database.

5. (Original) The fraud detection method according to claim 4, wherein the zip code is a ZIP + 4 zip code.

6. (Previously Presented) The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises comparing the city and state of the ship-to address against the city and state with a ZIP + 4 code.

7. (Previously Presented) The fraud detection method according to claim 1 wherein the step of checking the purchaser's ship-to address against criteria comprises the area code of the purchaser's phone number to determine whether it fits the geographic area of the ship-to address.

8. (Previously Presented) The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises comparing the purchaser's ship-to address against the national change of address service database or the publisher's change of address database.

9. (Previously Presented) The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises rating a building site associated with the "ship-to" address to determine whether the building or lot type is inconsistent with the transaction data.

10. (Previously Presented) The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of checking the purchaser's ship-to address against an historical database to determine whether a prior history of fraud exists.

11. (Original) The fraud detection method according to claim 10, wherein the prior history of fraud determining step comprises checking whether a record associated with the purchaser's ship-to address exists in the historical fraud database.

12. (Original) The fraud detection method according to claim 11, wherein the associated record is checked to determine whether negative data is associated with the ship-to address.

13. (Previously Presented) The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of checking the purchaser's ship-to address against an historical database to determine whether a pattern of fraudulent activity exists for the ship-to address.

14. (Original) The fraud detection method according to claim 13, wherein the pattern of fraud detecting step comprises determining whether an overlapping use of payment means and ship-to address is present by consulting a database of prior transactions.

15. (Original) The fraud detection method according to claim 13, wherein the pattern of fraud detecting step comprises retroactively notifying the merchant of previous transactions associated with the ship-to address once a pattern of fraudulent activity has been detected.

16. (Previously Presented) The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends.

17. (Previously Presented) The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of calculating a score based at least in part upon the likelihood that the transaction is fraudulent.

18. (canceled)

19. (canceled)

20. (canceled)

21. (canceled)

22. (canceled)

23. (canceled)

24. (canceled)

25. (canceled)

26. (canceled)

27. (canceled)

28. (canceled)

29. (canceled)

30. (canceled)

31. (canceled)

32. (canceled)

33. (Currently Amended) A system for detecting fraud in a non-personal environment involving shipment of physical merchandise from a merchant to a potential purchaser and, comprising:

a non-transitory computer usable medium having computer readable program code embedded therein ~~for detecting~~, when executed by a computer, causes the computer to detect fraud in a non-personal environment involving a potential purchaser and a merchant, the computer usable medium comprising:

computer readable program code for collecting purchaser data for a transaction, said purchaser data comprising a billing address and a ship-to address;

computer readable program code for transmitting said ship-to address to a fraud-detection system;

computer readable program code for processing said ship-to address to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to address against non-billing address criteria; and

computer readable program code for returning the relative risks of fraudulent activity associated with the transaction, and

whereby the shipment of the merchandise from the merchant to the purchaser is effected if the fraud detection system indicates that the relative risks of fraudulent activity associated with the transaction is below the merchant's threshold.

34. (Currently Amended) A method for detecting fraud in a non-personal environment involving shipment of physical merchandise from a merchant to a potential purchaser, comprising the steps of:

receiving and storing identity data of the potential purchaser on a non-transitory computer readable storage medium for processing interactively and in real-time on a computer, the identity data comprising a 'ship to' address of the potential purchaser;

parsing the 'ship to' address to postal standards with the computer processor and comparing the 'ship to' address against a Coding Accuracy Support System (CASS) to determine whether the 'ship to' address is a structurally viable and a deliverable address;

automatically prompting the purchaser to correct the 'ship to' address using a computer interface of the computer processor if the 'ship to' address is determined to be an unidentifiable addresses;

evaluating the results of the parsing and correcting steps to establish the relative risks of fraudulent activity associated with the transaction; and

wherein the shipment of the merchandise from the merchant to the purchaser is effected if the relative risks of fraudulent activity associated with the transaction is below the merchant's threshold.

35. (Previously Presented) The fraud detection method according to claim 34, wherein the step of checking the potential purchaser's 'ship-to' address further comprises checking to determine whether the potential purchaser's 'ship-to' address exists in the real world and modifying the likelihood that the transaction is fraudulent based on the results.

36. (Previously Presented) The fraud detection method according to claim 34 wherein the step of checking the potential purchaser's 'ship-to' address further comprises comparing a zip code of the 'ship-to address' against a post office database and comparing the city and state of the 'ship-to' address against a city and state represented by a ZIP + 4 code and modifying the likelihood that the transaction is fraudulent based on the results.

37. (Previously Presented) The fraud detection method according to claim 34, wherein the identity data further comprises the potential purchaser's area code and the 'ship-to' address checking step comprises checking the area code to determine whether the area code fits the geographic area of the purchaser's 'ship-to' address and modifying the likelihood that the transaction is fraudulent based on the results.

38. (Previously Presented) The fraud detection method according to claim 34, wherein the step of checking the potential purchaser's 'ship-to' address further comprises comparing a 'bill-

to' address against a change of address service database and modifying the likelihood that the transaction is fraudulent based on the results.

39. (Previously Presented) The fraud detection method according to claim 34, wherein the step of checking the potential purchaser's 'ship-to' address comprises rating a building site associated with the 'ship-to' address to determine whether the building or lot type is consistent with the transaction data and modifying the likelihood that the transaction is fraudulent based on the results.

40. (Previously Presented) The fraud detection method according to claim 34, wherein the step of checking the potential purchaser's 'ship-to' address further comprises checking the 'ship-to' address against an historical database to determine whether a prior history of fraud exists at the 'ship-to' address is and modifying the likelihood that the transaction is fraudulent based on the results.

41. (Previously Presented) The fraud detection method according to claim 40, wherein the step of checking the potential purchaser's 'ship-to' address further comprises checking a 'bill-to' address against an historical database to determine whether a prior history of fraudulent activity exists for the 'bill-to' address and modifying the likelihood that the transaction is fraudulent based on the results.

42. (Previously Presented) The fraud detection method according to claim 34, wherein the pattern of fraud detecting step further comprises determining whether an overlapping use of ship-

to addresses and payment means is present by consulting a database of recent prior transactions creating interlocking concurrent shipments to two or more addresses with three or more payment means, within a short period of time and the likelihood that the transaction is fraudulent based on the results.

43. (Previously Presented) The fraud detection method according to claim 42, wherein the pattern of fraud detecting step further comprises retroactively notifying merchants of previous transactions associated with the 'ship-to' address once a pattern of potential fraudulent activity has been detected, and modifying the likelihood that the transaction is fraudulent based on the results.

44. (Previously Presented) The fraud detection method according to claim 34, further comprising the step of checking the 'ship-to' address against a modeling engine to determine whether elements exist in the demographic data which correlate with recent fraud trends, and modifying the likelihood that the transaction is fraudulent based on the results.

45. (Previously Presented) A system for detecting fraud in a non-personal environment involving a potential purchaser and a merchant, comprising:

a non-transitory computer usable medium having computer readable program code embedded therein, when executed by a computer to detect fraud in a non-personal environment involving a potential purchaser and a merchant, the computer usable medium comprising:

computer readable program code for receiving and storing identity data of the potential purchaser for processing interactively and in real-time, the identity data comprising a 'ship to' address of the potential purchaser;

computer readable program code for parsing the 'ship to' address to postal standards with the computer processor and comparing the 'ship to' address against a Coding Accuracy Support System (CASS) to determine whether the 'ship to' address is a structurally viable and a deliverable address;

computer readable program code for automatically prompting the merchant to correct the 'ship to' address using a computer interface of the computer processor if the 'ship to' address is determined to be an unidentifiable addresses; and

computer readable program code for evaluating the results of the parsing and correcting steps to establish the relative risks of fraudulent activity associated with the transaction; and

whereby the shipment of the merchandise from the merchant to the purchaser is effected if the fraud detection system indicates that the relative risks of fraudulent activity associated with the transaction is below the merchant's threshold.